UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
NORTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

ANTHONY DEMASI,

Defendant.
_____/

Case No. 1:22-cr-20670

Honorable Thomas L. Ludington
United States District Judge

OPINION AND ORDER DENYING DEFENDANT'S MOTION TO SUPPRESS

Defendant Anthony Demasi is currently charged with three counts of bank fraud and three counts of aggravated identity theft for an alleged scheme in which he used the personal identification information of three of his student interns without their knowledge or consent to apply for credit cards in their names to defraud three different banks.

But this is not the first time Defendant has faced financial fraud allegations. Aside from a 2010 conviction in the Northern District of Illinois, a 2018 search warrant and incorporated affidavit alleged that Defendant impersonated two individuals by hacking into their email accounts and directing their accountants or assistants to wire money to Defendant's corporate accounts. The 2018 warrant authorized the seizure of all "records kept on paper and on digital devices" from the building which housed Defendant's businesses. Defendant seeks to suppress all evidence seized from the subsequent 2018 search *in this case* because he argues the 2018 warrant was unconstitutionally overbroad. Although this Court concludes the 2018 search warrant violated the Fourth Amendment's particularity requirement because it could have specified relevant dates or types of records to be seized, the inevitable discovery exception to the exclusionary rule applies and renders suppression inappropriate. Thus, Defendant's Motion will be denied.

I.

A.

Defendant Anthony Demasi currently faces a six-count Superseding Indictment charging three counts of bank fraud in violation of 18 U.S.C. § 1344(1) (Counts I, III, and V) and three counts of aggravated identity theft in violation of 18 U.S.C. § 1028A(a)(1) (Counts II, IV, and VI) for three different schemes to defraud three different banks by filing false credit card applications using the names, birthdates, and Social Security numbers of three different people without their knowledge or consent. ECF No. 21.

According to the Superseding Indictment, the first alleged scheme began on January 4, 2018, when Defendant submitted a credit card application to Barclays Bank Delaware (Barclays) using "Person A's" identification information. *Id.* at PageID.77–79. The second alleged scheme began on March 6, 2018, when Defendant submitted another false credit card application to JP Morgan Chase Bank NA (Chase) using "Person B's" identification information. *Id.* at PageID.79–80. The third and final alleged scheme began on August 31, 2018, when Defendant submitted yet another false credit card application to Capital One Bank NA (Capital One) using "Person C's" identification information. *Id.* at PageID.81–82. As a part of this scheme, the Government alleges that Defendant impersonated at least one of these victims in phone conversations with the bank he allegedly sought to defraud. ECF No. 32 at PageID.151.

Persons A, B, and C were students hired by Defendant to work or intern for his businesses between late 2017 and early 2018 who gave Defendant their personal identification information while interviewing and onboarding for their internship.[1] ECF No. 40 at PageID.239–40.

[1] Defendant argues that Persons A, B, and C were not all student-interns while working for Defendant's businesses. ECF No. 50 at PageID.344.

Defendant allegedly filed a credit card application with Barclays using Person A's identification information while Person A was interning for Defendant. ECF No. 32 at PageID.152. The same day Defendant filed the application, he emailed "Person A that he added her name to an existing office Barclays account" and told her to bring him the credit card when it arrived. *Id.* Person A did so, and although Defendant eventually returned the card, Defendant never provided the PIN, so Person A was unable to access the account.[2] *Id.* But Defendant could access the account, and the Government alleges he charged $3,969.79 to the card issued in Person A's name. *Id.* Person A became aware of the charges one month later when she checked her credit score. *Id.*

The credit card application Defendant allegedly falsely submitted in Person B's name was denied. *Id.* at PageID.153. On March 7, 2018, Person B discovered this denial—and the credit card application—when she received a letter from Chase informing her that an application for a credit card in her name had been denied. *Id.*

Person C stopped working for Defendant in the first week of August 2018. *Id.* at PageID.154. But, on August 31, 2018, Defendant allegedly used Person C's identification information to apply for a credit card with Capital One. *Id.* This application was approved but Person C did not know about the application until he was notified by a credit reporting service that he owed over $9,700 on a credit card account he knew nothing about and did not authorize. *Id.*

At a Suppression Hearing held on December 6, 2023, the Government identified two of these victims: Samantha May Berryhill and Carlie Zarkowski. ECF No. 48 at PageID.331. Defendant identified the third victim as Jake Peters. ECF No. 50 at PageID.348.

[2] Defendant concedes that he emailed Person A and added her to the Barclays account but maintains he never told Person A to bring him the card upon arrival and that Person A had access to the account. ECF No. 50 at PageID.344.

On October 17, 2023, Defendant filed a Motion to Suppress all evidence seized during a 2018 search of the building associated with his businesses, even though the schemes detailed in the affidavit supporting the 2018 search are unrelated to the charges in the instant Superseding Indictment. *See* ECF No. 36. The 2018 search, and its relation to the instant charges and Defendant's 2023 Motion to Dismiss, are discussed in greater detail below.

B.

On August 30, 2018, Agent Bryan Butler[3] of the Federal Bureau of Investigations (FBI) applied for a warrant to search Suite 8 of 1234 E. Broomfield Street in Mount Pleasant, Michigan ("Suite 8")[4] for evidence that Defendant committed wire fraud, financial institution fraud, and conspiracy. ECF No. 36-1 at PageID.206–07. His affidavit detailed the following:

In March 2010, Defendant pled guilty to three counts of wire fraud and two counts of securities fraud in the Northern District of Illinois. *Id.* at PageID.208. Defendant moved to Michigan after serving a five-year prison sentence. *See id.* After his release, in January of 2016, Defendant worked with David Coker, Jr. to organize the following corporate entities: (1) Goldman Advisors, LLC (Goldman);[5] (2) Hoya Capital Management, LLC (HCM);[6] (3) Beta Sole Foundation;[7] and (4) Virtue Venture Group, LLC.[8] *Id.* Although separate entities, Defendant

[3] Agent Butler has been employed by the FBI since 2009 and specializes in fraud investigations. *See* ECF No. 36-1 at PageID.207.

[4] The building at 1234 Broomfield is a one-story business complex with multiple suites and a common parking lot. *See* ECF No. 36-1 at PageID.217–18. Suite 8 was leased by one of corporate entities Defendant served as a principal of, but a copy of the lease—which would confirm Defendant's standing to seek suppression—has not been produced.

[5] Defendant describes Goldman as a consulting company which would give "general business advice to other business in their general business plan." *See* ECF No. 48 at PageID.332 n. 3.

[6] Defendant describes HCM as a company "designed to raise capital for other businesses." *See* ECF No. 48 at PageID.332 n. 4.

[7] Defendant describes Beta Sole Foundation as a 501(c)(3) focused on "educational principles."

[8] Defendant describes Virtue Venture, LLC as a product development company. *See* ECF No. 48 at PageID.332 n. 5.

served as a principal for each. ECF No. 48 at PageID.332. And Each entity used Suite 8 for office space and evidence suggests that Suite 8 was each entity's principal place of business. *See* ECF No. 36-1 at PageID.208, 214. Suite 8 was an open and common floor plan in which, "at one work station, somebody would be doing the work of one of the entities [and] at the next work station somebody else would be doing the work of" another entity. ECF No. 48 at PageID.332.

Each entity had separate bank accounts, though. On April 13, 2016, Coker opened a bank account for HCM with Fifth Third Bank. ECF No. 36-1 at PageID.209. The account number ended in 4070 and Defendant was added as a signatory on May 30, 2017. *Id.*

On November 7, 2017, Wendi Paschal received an email seemingly sent by Michael Gunn, while working for Gunn as his personal assistant. *Id.* "The email directed Paschal to wire $200,000 from Gunn's [bank] account" to HCM's account ending in 4070. *Id.* After Paschal replied to the email asking for clarification, and after she received a second email seemingly sent by Gunn asking her to initiate the wire transfer to HCM, she did so. *Id.* at PageID.209–10. Immediately before this wire transfer, the HCM account had a negative balance. *Id.* at PageID.211.

Gunn learned of the transfer the following day when a credit union representative informed him of the suspicious activity. *Id.* at PageID.210. Gunn denied emailing Paschal and claimed he "never heard of" HCM. *Id.* After speaking with Paschal about the emails, Gunn discovered filters on his email account which directed any email containing the word "wire" to Gunn's "deleted items folder." *Id.* at PageID.210–11. Gunn denied installing these filters and told Agent Butler he "had no prior knowledge of what filters were[.]" *Id.* at PageID.211.

After the HCM account received the wire transfer, several withdraws were made. *See id.* At least two withdraws were made by a debit card issued to Defendant, totaling $806. *See id.* at PageID.211–12. On November 8, 2017, Defendant also allegedly purchased $6,000 in cashier's

checks, and withdrew an additional $2,000 in cash from a local bank. *Id.* at PageID.212. On November 9, 2017, Defendant's debit card was used to make three purchases from Godaddy.com. *Id.* At some point after November 9, 2017, HCM's bank returned $170,849 from HCM's account to Gunn's. *Id.* Accordingly, Gunn lost approximately $29,151 as a result of the wire transfer. *Id.*

But Gunn was not the only individual allegedly targeted by this November 7, 2017 email scheme. That same day, Sherley Matteson's accountant, Andrea Carlson, received an email seemingly sent by Matteson, asking Carlson to initiate a wire transfer. *Id.* at PageID.212–13. Carlson replied and received a response—again seemingly sent by Matteson—directing Carlson to wire $176,000 to the HCM bank account ending in 4070. *Id.* at PageID.213. But Carlson did not initiate the transfer because, when she called Matteson to confirm, Matteson said she had "no idea" what Carlson was talking about. *Id.* Like Gunn, Matteson also allegedly discovered that filters were placed on her email account which directed all emails from Carlson to Matteson's trash folder. *Id.* And, like Gunn, Matteson had never heard of HCM. *Id.*

Throughout his investigation, Agent Butler surveilled Defendant and 1234 Broomfield St. in January 2018. *See id.* at PageID.214–15. As a part of his surveillance, Agent Butler was allowed inside the building and Suite 8 and noted that all entities within Suite 8 (HCM, Goldman, Virtue Venture, and Beta Sole) "share in common the use of the office space."[9] *Id.* at PageID.215.

Based on the investigation detailed above, the 2018 warrant sought "records kept on paper and on digital devices, such as computers, cellular telephones and digital storage media, and devices used to access financial accounts, such as ATM, debit and credit cards, and account

[9] This is disputed. At the suppression hearing, Defendant argued that "things were kept separate" in Suite 8 and there were "three separate sections" devoted to Goldman, Beta Sole, and HCM. After the suppression hearing, Defendant argued all employees for all businesses "worked in separate workspaces. Moreover, files for the business[es] were maintained separately, and there were separate computers for the . . . businesses with separate drives." ECF No. 50 at PageID.345.

identification cards, and safety deposit box keys." *Id.* at PageID.215, 219. Agent Butler claimed these records would likely contain: (1) evidence regarding who has access to the digital devices and the financial accounts used by the various entities and individuals; (2) photographic images of people in association with each other; (3) communications with co-conspirators, victims, and third parties; (4) information regarding financial transactions; (5) corporate activity records; (6) contact lists; (7) information regarding the location and disposition of the proceeds of the fraud scheme; and (8) on the digital devices, records of online activity. *Id.* at PageID.215–16. Magistrate Judge Patricia T. Morris authorized the search warrant on August 30, 2018. *Id.* at PageID.220. At 6:17 PM on September 5, 2018, Agent Bryan Butler and company searched Suite 8 and seized 31 categories of evidence, including various documents and records. *See id.* at PageID.225–27.

C.

Returning to Defendant's 2023 Motion to Suppress, Defendant now seeks to suppress evidence seized during the 2018 search in *this* case, arguing that the 2018 search warrant was unconstitutionally overbroad because it authorized the general seizure of records within Suite 8 with no limitation on relevant dates, business entities, or subject matter. ECF No. 36 at PageID.200–04.

The Government responds, as a threshold matter, that the only evidence seized in 2018 that it intends to use at trial is a single sheet of paper containing the name, birthdate, and social security number of May Berryhill—a victim of Defendant's alleged credit card scheme—which was discovered throughout the instant investigation *months* after it was seized in 2018 in connection to Defendant's alleged email schemes. *See* ECF No. 41 at PageID.249. And the Government further notes it will only use this piece of paper to corroborate Berryhill's testimony that she provided her

identification information to Defendant while interviewing and onboarding for her employment. ECF No. 48 at PageID.335.

The Government argues that the search was not overbroad given the sophisticated nature of the financial fraud described in the 2018 search affidavit and the communal nature of Defendant's business entities. ECF No. 41 at PageID.250–56. The Government also argues that, even if the 2018 search warrant was overbroad, both the good-faith exception and the inevitable discovery exception to the exclusionary rule apply, rendering suppression inappropriate. *Id.* at PageID.256–58.

II.

The Fourth Amendment guarantees that "no [w]arrants shall issue, but upon probable cause, supported by [o]ath or affirmation, and *particularly* describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV (emphasis added). Violations of the Fourth Amendment—including this particularity requirement—may result in suppression of tainted evidence under the exclusionary rule, absent attenuation or exception. *United States v. Galaviz*, 645 F.3d 347, 354 (6th Cir. 2011); *see also United States v. Waide*, 60 F.4th 327, 338 (6th Cir. 2023) ("Courts are required to suppress evidence that is directly or indirectly 'the tainted fruit' of unlawful government conduct.'" (quoting *Nix v. Williams*, 467 U.S. 431, 441 (1984))).

III.

A. Fourth Amendment Violation: Particularity and Overbreadth

This Court begins, therefore, by analyzing whether the 2018 warrant violated the Fourth Amendment in the first instance. Defendant argues the 2018 search warrant violated the Fourth Amendment's particularity requirement by authorizing the seizure of *all* records in Suite 8, even though only one of Defendant's businesses located there—HCM—was tied to the alleged email

schemes in Agent Butler's affidavit. ECF Nos. 36 at PageID.200–04; 42 at PageID.277–82. Although the warrant was as specific as it could have been as to which businesses' records were to be seized, the warrant was insufficiently specific as to the *date* and *type* of relevant records to be seized and, thus, is overbroad.

The Fourth Amendment particularity requirement demands that warrants describe with particularity the place to be searched and the things to be seized "to prevent the seizure of one thing under a warrant describing another in violation of the Fourth Amendment." *United States v. Richards*, 659 F.3d 527, 537 (6th Cir. 2011) (quoting *United States v. Wright*, 343 F.3d 849, 863 (6th Cir.2003)). "The chief purpose of the particularity requirement [is] to prevent *general* searches by requiring a neutral judicial officer to cabin the scope of the search to those areas and items for which there exists probable cause that a crime has been committed." *Baranski v. Fifteen Unknown Agents of the Bureau of Alcohol, Tobacco and Firearms*, 452 F.3d 433, 441 (6th Cir.2006) (emphasis added). If the particularity requirement is not satisfied, the warrant is unconstitutionally overbroad in violation of the Fourth Amendment.

The "degree of specificity required" to satisfy the particularity requirement is "flexible and will vary depending on the crime involved and the types of items sought," *United States v. Richards*, 659 F.3d 527, 537 (6th Cir. 2011) (quoiting *United States v. Greene*, 250 F.3d 471, 477 (6th Cir. 2001)). "Consequently, a description is 'valid if it is as specific as the circumstances and the nature of the activity under investigation permit.'" *Green*, 250 F.3d at 477 (quoting *United States v. Ables*, 167 F.3d 1021, 1033 (6th Cir. 1999)). Importantly, this specificity may be satisfied by a search warrant affidavit which the warrant itself expressly incorporates. *Richards*, 659 F.3d at 537; *Groh v. Ramirez*, 540 U.S. 551, 557 (2004).

Here, the 2018 search warrant expressly incorporated Agent Butler's warrant application and attached affidavit, which was reviewed and signed by Judge Morris. *See* ECF No. 36-1 at PageID.206, 207–16, 220. The warrant described the things to be seized as:

> [(1)] Records kept on paper and on digital devices, such as computers, cellular telephones and digital storage media, and [(2)] devices used to access financial accounts, such as ATM, debit and credit cards, and account identification cards, and safety deposit box keys.

Id. at PageID.219–20.

Although a close call, the 2018 warrant authorized a broader search than was reasonable given the facts in Agent Butler's affidavit. First, the 2018 warrant did not place any *temporal* limitation on the records to be seized. Agent Butler's affidavit described an investigation beginning in 2016 which involved alleged email schemes in November 2017. *See* ECF No. 36-1 at PageID.208–16. But the warrant does not specify any relevant timeframe during which the "records kept on paper and on digital devices" sought to be seized may have been relevant. This "failure to limit broad descriptive terms by relevant dates, when such dates are available to the police, . . . render[s] a warrant overbroad." *United States v. Ford*, 184 F.3d at 566 (6th Cir. 1999) (*citing United States v. Cardwell*, 680 F.2d 75, 78 (9th Cir.1982) and *United States v. Abrams*, 615 F.2d 541, 545 (1st Cir.1980) ("A time frame should also have been incorporated into the warrant.")); *see also United States v. Abboud*, 438 F.3d 554, 576 (6th Cir. 2006) (holding a warrant in a financial fraud case was unconstitutionally overbroad because it sought the seizure of records from as early as 1996 when the affidavit did not allege criminal activity until 1999).

Second, the 2018 warrant did not specify what *types* of records were relevant. The Sixth Circuit has recognized the common-sense notion that "once a category of seizable papers has been adequately described . . . the Fourth Amendment is not violated" simply "because the officers executing the warrant must exercise some minimal judgement as to whether a particular document

falls within the desired category." *United States v. Blair*, 214 F.3d 690, 697 (6th Cir. 2000) (internal quotations omitted). But the 2018 warrant did not delineate a category of relevant records and instead authorized the seizure of *all* "[r]ecords kept on paper and on digital devices[.]" ECF No. 36-1 at PageID.219. This missing categorization is critical. Indeed, in all cases the Government relies on to argue the 2018 warrant was sufficiently specific, the warrants identified *some* relevant aspect of the to-be-seized records which served as a nexus to the allegations within the warrant application. *See, e.g.*, *Blair*, 214 F.3d 690 (finding warrant sufficiently specific when describing items to be seized as "[b]ooks, records, receipts, notes, ledgers . . . and other papers *relating to the transportation, importation, ordering, sale, and distribution of controlled substances*." (emphasis added)); *United States v. Logan*, 250 F.3d 350, 366 (6th Cir. 2001) (finding warrant sufficiently specific when describing items to be seized as "[r]ecords, files, documents, notes, correspondence, microfiche, or computerized entries *concerning the Department of Housing and Urban Development (HUD), Government National Mortgage Association (GNMA), Federal Housing Administration (FHA) . . . and copies of submissions to FHA, GNMA, HUD, FHA insurance claims and claims records*." (emphasis added)). Had the 2018 search warrant simply cabined the "records kept on paper and digital devices" to those records related to the wire and financial fraud alleged in Agent Butler's warrant affidavit, the Fourth Amendment particularity requirement likely would have been satisfied. Instead, the warrant authorized police to seize literally all records within Suite 8. This overbreadth violates the Fourth Amendment.

Before turning to whether this overbreadth requires suppression under the exclusionary rule, it is important to note that, contrary to Defendant's argument, the warrant was as specific as it could have been concerning which of Defendant's business entities' records should have been seized. *See* ECF No. 36 at PageID.201–04 (arguing 2018 warrant was overbroad because it was

not limited to HCM's records). Agent Butler averred that, based on his own surveillance of the building, Suite 8 was a common space shared by all of Defendant's business entities, including HCM. ECF No. 36-1 at PageID.215.Agent Butler's affidavit also noted that these business often operated interchangeably. *See id.* at PageID.212 (noting Defendant withdrew from HCM's bank account to make three purchases on Godaddy.com, which provided the domain for Goldman and Beta Soul), PageID.214 (noting someone from HCM submitted a form to a bank listing the entity's name as "Goldman Advisors Group"). Accordingly, the 2018 warrant was as specific as it could have been under the circumstances in terms of *whose* records were to be seized—as records corroborating Defendant's alleged financial and wire fraud could have reasonably been found in *any* portion of Suite 8, relating to *any* of his business entities.

B. The Exclusionary Rule

Having determined that the 2018 search warrant violated the Fourth Amendment's particularity requirement, this Court turns to the proper remedy. Although "[t]he Fourth Amendment protects the right to be free form 'unreasonable searches and seizures,'" it is "silent about how this right is to be enforced." *Davis v. United States*, 564 U.S. 229, 231 (2011). Accordingly, the Supreme Court created the "exclusionary rule," as a "deterrent sanction that bars the prosecution from introducing evidence obtained by way of a Fourth Amendment violation."[10]

[10] Notably, under the "fruit of the poisonous tree" doctrine, which supplements the exclusionary rule, only those pieces of evidence—the fruits—which *derive* from the constitutional violation—the poisonous tree—are suppressed, absent attenuation. *See United States v. Pearce*, 531 F.3d 374, 381 (6th Cir. 2008). Recall the Government asserts only one "fruit" of the 2018 search will be used at Defendant's trial on the instant charges: a single sheet of paper showing that Berryhill provided her name, birthdate, and social security number to Defendant throughout her employment onboarding. *See* ECF No. 41 at PageID.249. Thus, to the extent suppression is warranted and no exception to the exclusionary rule applies, the only piece of evidence that would be suppressed at trial is this single sheet of paper. Although Defendant argues there are many more "fruits" of the unconstitutional 2018 search, ECF No. 42 at PageID.284–85, none are evident to this Court upon review of the record and the December 2023 suppression hearing.

Id. This rule is not rigid. Indeed, the Supreme Court has created several exceptions to the exclusionary rule when suppressing evidence obtained in violation of the Fourth Amendment would do "nothing to deter police misconduct." *See id.* When these exceptions apply, even if a defendant's Fourth Amendment right has been violated, suppression is not the right remedy. The Government argues that both the good faith and inevitable discovery exceptions apply. ECF Nos. 41 at PageID.256–58; 49 at PageID.339–40. Both exceptions will be addressed in turn.

1. Good Faith Exception

One exception to the Fourth Amendment exclusionary rule—known as the "good faith" exception—applies when the officer who conducted the search acts in objectively reasonable reliance on a subsequently invalidated warrant. *United States v. Soto*, 794 F.3d 635, 646 (6th Cir. 2015) ("Courts do not suppress evidence that officers 'obtain in objectively reasonable reliance on a subsequently invalidated search warrant.'" (quoting *United States v. Leon*, 468 U.S. 897, 922 (1984))). The good faith exception was created by the Supreme Court in 1984 in *United States v. Leon*.[11] The Sixth Circuit has instructed, following *Leon*, that courts presented with a motion to suppress alleging a flawed warrant must ask "whether a reasonably well[-]trained officer would have known that the search was illegal despite the magistrate's decision. Only when the answer is 'yes' is suppression appropriate." *United States v. White*, 874 F.3d 490, 496 (6th Cir. 2017) (internal citations omitted). When answering this question, this Court is limited to the "four corners

[11] In *Leon,* the Supreme Court found that the exclusionary rule's rationale—to deter unlawful police conduct—does not apply in situations when an officer acts in objectively reasonable reliance on a warrant because "there is no police illegality and thus nothing to deter." *United States v. Leon*, 468 U.S. 897, 921 (1984). The Court emphasized that "[p]enalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." *Id.*

of the [search] affidavit." *United States v. Hython*, 443 F.3d 480, 487 (6th Cir. 2006) (citing *United States v. Laughton*, 409 F.3d 744, 751 (6th Cir.2005)).

The good faith exception to the exclusionary rule is a broad one. Only four circumstances exist where the exception will *not* apply: "(1) where the issuing magistrate was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard for the truth; (2) where the issuing magistrate wholly abandoned his judicial role and failed to act in a neutral and detached fashion, serving merely as a rubber stamp for the police; (3) where the affidavit was nothing more than a "bare bones" affidavit that did not provide the magistrate with a substantial basis for determining the existence of probable cause, or where the affidavit was so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) where the officer's reliance on the warrant was not in good faith or objectively reasonable, such as where the warrant is facially deficient." *United States v. Lewis*, No. 22-5593, 2023 WL 5665548 (6th Cir. Sept. 1, 2023) (quoting *United States v. Rice*, 478 F.3d 704, 712 (6th Cir. 2007).

Here, nothing suggests that Agent Butler knowingly submitted a false affidavit or otherwise acted in bad faith when seeking the search warrant. The warrant was issued by a proper authority—a United States Magistrate Judge—and nothing suggests the magistrate judge abandoned her neutral role when authorizing the warrant. *See* ECF No. 36-1 at PageID.220. Further, the warrant, which incorporated Agent Butler's affidavit, was not "bare bones" and provided the magistrate with a substantial basis to determine whether probable cause existed concerning Defendant's alleged wire fraud and email schemes. *See id.* at PageID.207–16. However, warrants that are constitutionally overbroad for lacking particularity in defining the place to be searched and things to be seized are textbook examples of *facially deficient* warrants which officers cannot reasonably

rely on in good faith. *United States v. Leon*, 468 U.S. 897, 924 (1984) ("[A] warrant may be so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonable presume it to be valid."); *see also Groh v. Ramirez*, 540 U.S. 551, 565 (2004) (noting good faith exception to exclusionary rule does not apply to overbroad warrants which violate the Fourth Amendment particularity requirement). Accordingly, the good faith exception to the exclusionary rule does not apply to this case involving a facially deficient, unconstitutionally overbroad warrant.[12]

2. Inevitable Discovery Exception

Unlike the good-faith exception to the exclusionary rule, the inevitable discovery exception applies here and renders suppression—of the sole sheet of paper the Government intends to use from the 2018 search at Defendant's trial—inappropriate.

The inevitable discovery exception to the exclusionary rule applies when the Government can demonstrate, by a preponderance of the evidence, either (1) "the existence of an independent, untainted investigation that inevitably would have uncovered the same evidence[;]" or (2) "other compelling facts establishing that the disputed evidence inevitably would have been discovered." *United States v. Bost*, 606 F. App'x 821, 827 (6th Cir. 2015) (internal citations omitted). When analyzing the applicability of this exception, this Court must "determine, viewing affairs as they

[12] The Government argues that the Supreme Court's 2009 decision in *Herring v. United States*, 555 U.S. 135 (2009) alters the analysis. But that case is not applicable here. In *Herring*, a man sought to retrieve an item from his impounded truck when officers discovered an outstanding warrant for his arrest and accordingly searched him, seizing drugs and unlawful firearms from his person. *Id.* at 137–39. However, officers later discovered that the arrest warrant had been withdrawn. *Id.* The Supreme Court denied suppression and held that, to justify exclusion, police error must be "deliberate, reckless, or grossly negligent." *Id.* at 144. But the Sixth Circuit has since held that *Herring* "does not . . . alter that aspect of the exclusionary rule which applies to warrants that are facially deficient" and affirmed suppression of evidence seized from an unconstitutionally overbroad warrant, despite no evidence that officers acted recklessly or deliberately. *United States v. Lazar*, 604 F.3d 230, 237 (6th Cir. 2010).

existed at the instant before the unlawful search, what would have happened had the unlawful search never occurred." *United States v. Kennedy*, 61 F.3d 494, 498 (6th Cir. 1995). This exception exists because, when evidence "ultimately or inevitably would have been discovered by lawful means," the exclusionary rule's deterrence rationale "has so little basis that the evidence should be received. Anything else would reject logic, experience, and common sense." *Nix v. Williams*, 467 U.S. 431, 444 (1984) (footnote omitted).

Here, the Government has demonstrated by a preponderance of the evidence that law enforcement would have inevitably and independently discovered Defendant's conduct giving rise to the 2022 indictment—Defendant's alleged credit card schemes—regardless of the constitutionality of the 2018 search of Suite 8 relating to Defendant's alleged email schemes. At the December 6, 2023 Suppression Hearing, the Government averred that one of Defendant's financial fraud victims in *this* case—Carlie Zarkowski—came forward voluntarily to report Defendant's financial fraud after she received a letter from Chase on March 7, 2018, informing her that a credit card application in her name—which she never filled out—was denied. ECF No. 48 at PageID.335–36.

Specifically, Carlie Zarkowski was a student at Central Michigan University (CMU) who interned for Defendant but left his employ in August of 2018 *before* the search of Suite 8. *Id.* at PageID.336. On August 14, 2018, after Zarkowski left Defendant's employ but before the search of Suite 8, Defendant emailed CMU staff expressing his dissatisfaction with Zarkowski as an intern. *See id.* Then, on September 4, 2018—the day before the search of Suite 8—Defendant emailed the same CMU staff member asking whether he could file a formal complaint against Zarkowski because "things did not work out" and she somehow "cost [his] business a lot of real dollars and has put [his] operations in jeopardy[.]" *Id.*

Two days later—the day after the 2018 search—Defendant received a response from Dr. Nailya Delellis—the director of CMU's undergraduate Health Administration Program—in which Dr. Delellis informed Defendant that his "formal complaint" should be filed with CMU Police and CMU's Office of Student Affairs, who Delellis included on the email. *Id.* On September 7, 2018, Zarkowski voluntarily went to the CMU Police Department for an interview with Detective Jason VanConant. *Id.* During the interview, Zarkowski voluntarily told Detective VanConant that a credit card was taken out in her name without her authorization while working for Defendant, and that she knew the FBI recently searched Suite 8. *Id.* Detective VanConant then contacted Agent Butler over the phone and told Butler about Zarkowski's report. *Id.* Agent Butler sent Detective VanConant a follow-up email indicating he would set up a "follow-up interview" between Zarkowski and the FBI, if VanConant provided her contact information, and that Butler would reach back out to VanConant to obtain a copy of Zarkowski's recorded CMU interview. *Id.* at PageID.336–37.

Defendant's current bank fraud and aggravated identity theft charges, ECF No. 21, were the result of an independent investigation, untainted by the lack of particularity in a search warrant issued three years prior concerning unrelated financial fraud. Indeed, as the Government notes, "ironically . . . it was . . . [Defendant]'s complaint to . . . CMU about Ms. Zarkowski that led to the discovery of the charged fraud in the instant case." ECF No. 49 at PageID.340. In sum, although the 2018 search warrant lacked particularity in describing the things to be seized and was thus unconstitutionally overbroad and facially deficient, the inevitable discovery exception to the exclusionary rule applies and renders suppression in this case inappropriate.

IV.

Accordingly, it is **ORDERED** that Defendant's Motion to Suppress, ECF No. 36, is **DENIED.**

This is not a final order and does not close the above-captioned case.

Dated: February 7, 2024

s/Thomas L. Ludington
THOMAS L. LUDINGTON
United States District Judge